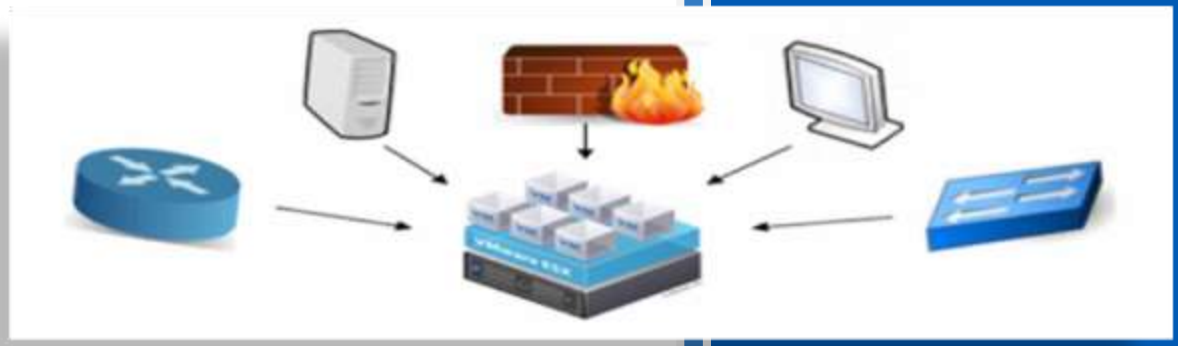
2013

Virtualized and Integrated Routing Project: Project Manual



Gerben Kleijn & Terence Nicholls

Pro 483

9/15/2013

Contents

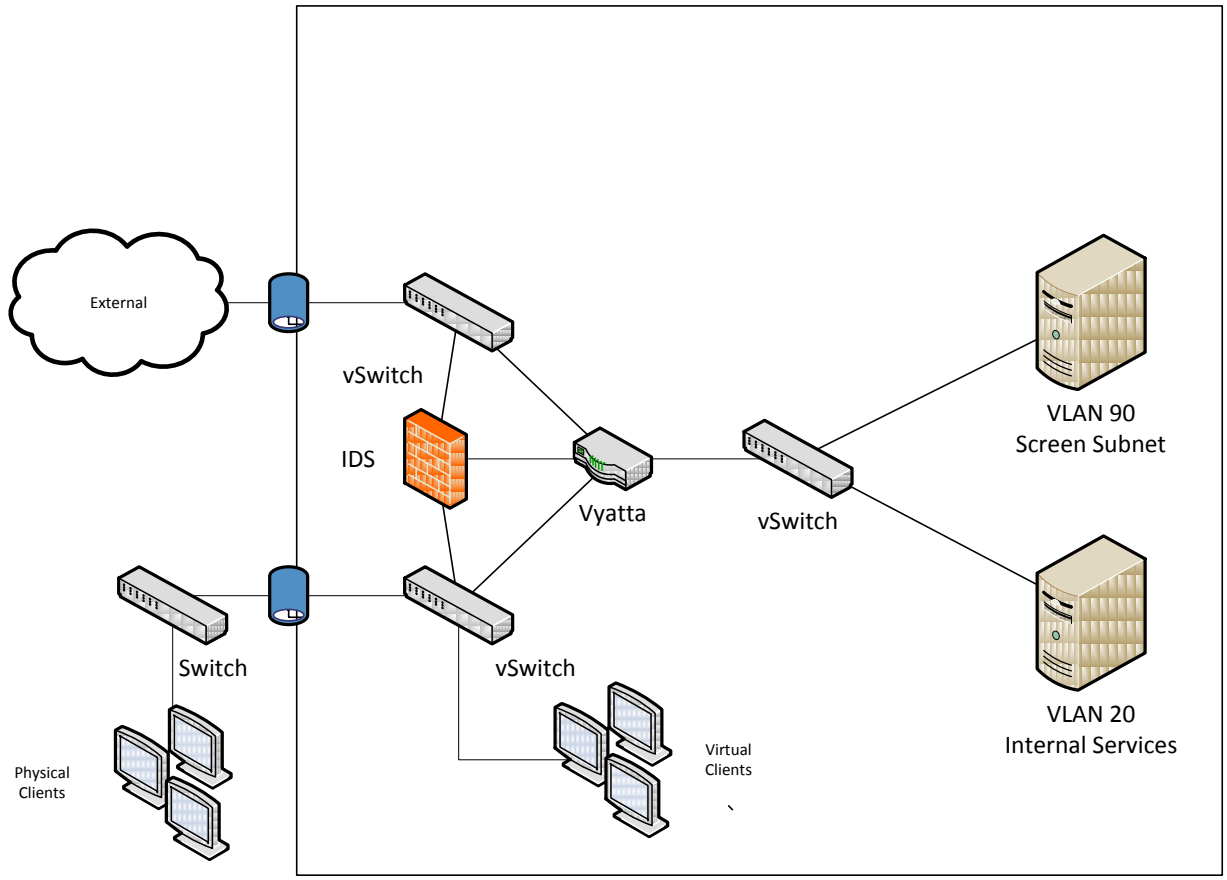
Quickstart Guide 3
Topology and Network Description 4
Device Information 5
Manual Network Configuration 5
Virtual Switch Configuration 7
NAT 7
Firewall Rules 8
Adding users to LDAP 9

Quickstart Guide

So you have just purchased a virtualized and integrated routing product. While the product allows for extensive customization, most users will just want to plug it in, hook it up, and get it to work. To do so, just follow these steps:

1. Power on the device
2. Plug a laptop into Ethernet adapter 1 (vmnic0) and open up vSphere. Enter the following information:
    a. IP address 10.0.0.2
    b. Username root
    c. Password gerbentjPLOK!
3. Once inside vSphere, open up 'VM's and Templates', and start up the vCenter virtual machine. You can watch the progress through the 'console' tab. Once it asks for a username and password you're done. There's no need to log in.
4. Disconnect vSphere and establish a new connection to vCenter.
    a. IP address 10.0.0.10
    b. Username root
    c. Password gerbentjPLOK!
5. Go to 'VM's and Templates' and power on all the virtual machines.
6. Once the Vyatta virtual machine is powered on, log in:
    a. Username vyatta
    b. Password gerbentjPLOK!
7. Change the IP address of vyatta's 'eth4' interface to the IP address that you received from your ISP through the following commands:
    a. 'configure'
    b. 'set interfaces Ethernet eth4 address [x.x.x.x/x]
    c. 'commit'
    d. 'save'
8. Plug your Internet connection into Ethernet adapter 2 (vmnic1).
9. Your network is now ready for use. Please study the network topology and device information in this user manual to find out about the servers and services on your virtual network. It is also strongly recommended to change all the default passwords found in the 'device information' section of this manual to something different.

Topology and Network Description



After following the steps in the quickstart guide your network is ready for use. However, you will want disconnect your laptop from Ethernet adapter 1 and attach a switch instead, so that more than one user can use the virtual network simultaneously. When any user attached to the network sends out information over the network, the information arrives at its final location through the following steps:

1. It arrives at the physical switch
2. If it is destined for another physical client, it will not enter the virtual environment.
3. If not, sends to information into the server.
4. If the information is meant for a virtual client, a vSwitch sends it to the virtual client's subnet.
5. For other destinations it still travels to the virtual switch first. The virtual switch sends the information to the virtual router, as well as to the virtual IDS (Intrusion Detection System) for security purposes.
6. The virtual router decides where the information needs to go:
    a. If the information contains a DNS request for a website on the internet, it is sent to VLAN 90 which contains the DMZ DNS server. Along the way it encounters another virtual switch that makes sure it is sent to the DMZ subnet rather than the Internal

Services subnet. The DMZ DNS server sends the DNS request out to the Internet and awaits a response, which is then sent back to the client.

b. If the information is meant for an internal virtual server, it is sent to VLAN 20. Along the way it encounters another virtual switch that makes sure it is sent to the Internal Services subnet rather than the DMZ subnet.
c. If the information is meant for the Internet, it is sent out through the Ethernet adapter 2, which should be connected to the Internet Service provider's connection.

7. The same principles apply for connections that are not established from the physical clients from the virtual clients or the virtual servers. Note that there are various access control lists in place that only allow specific services for security purposes. For more information on firewall rules, please review the 'firewall rules' section of this manual.

Device Information

For information on what servers are present on the virtual network and what their IP addresses, login information, and functions are please review the following table:

Server	IP Address	Username	Password	Function
vCenter	10.0.0.10	root	gerbentjPLOK!	Manages the ESXi host and virtual machines
vyatta	multiple	vyatta	gerbentjPLOK!	Virtual router and firewall
SIP-SRV-LDAPDNS	10.0.20.10	sipadmin	gerbentjPLOK!	LDAP and internal DNS server
SIP-SRV-NAS	10.0.20.21	sipadmin	gerbentjPLOK!	Data storage
SIP-DMZ-DNS	10.0.90.10	sipadmin	gerbentjPLOK!	External DNS server
SIP-CLIENT-WINDOWS	DHCP	.\sipuser	gerbentjPLOK!	Virtual client running Windows
SIP-CLIENT-LINUX	DHCP	.\sipuser	gerbentjPLOK!	Virtual client running Ubuntu
SIP-SEC-IDS	10.0.20.20	sipadmin	gerbentjPLOK	Network Monitoring

Manual Network Configuration

If you follow the quickstart guide, your virtual network will have several pre-configured IP address ranges. These settings will work for most small businesses, but if you wish to set up your own, personalized IP address ranges then the following settings on the virtual machines have to be configured:

1. The interfaces on Vyatta have to be configured with custom IP addresses
    a. Log into vyatta
    b. Enter configuration mode through the 'configure' command
    c. Delete the previously assigned IP addresses through the command 'delete interfaces Ethernet [interface] address [address]

    d. Enter a new IP address for the interface through the command ‘set interfaces Ethernet [interface] address [address]
    e. Commit the changes to working memory using the ‘commit’ command
    f. Save the changes to the configuration file using the ‘save’ command.
    g. Exit configuration mode through the ‘exit’ command
2. The servers and clients have to be provided with new IP addresses according to the new subnet layout. Below is some information on how to change IP addresses for the various operating systems that are in use on your virtual network:
    a. Windows:
        i. Click ‘start’ and open up the control panel.
        ii. Go to ‘network and Internet’ and select ‘change adapter settings’.
        iii. Right-click the network adapter for which you wish to change settings and select ‘properties’
        iv. Select ‘Internet Protocol Version 4’ and click ‘properties’.
        v. Enter the appropriate network settings and click ‘ok’.
    b. Linux Ubuntu:
        i. Click the settings wheel in the top right corner.
        ii. Select ‘System Settings’.
        iii. Select ‘Network’.
        iv. Select ‘Options’.
        v. Select the ‘IPv4 Settings’ tab.
        vi. Enter the appropriate network settings and click ‘Save’.
    c. Zentyal:
        i. Open up the web-based dashboard
        ii. Click on ‘network’ and then ‘Interfaces’.
        iii. Select the interface for which you wish to make changes.
        iv. Apply the appropriate changes and click ‘change’.
        v. Click ‘save changes’ at the top right of your screen.

If you wish to not only assign custom IP address ranges but also to change the network subnets that certain devices are connected to, then the following steps have to be taken:

1. Select the virtual machine in vSphere and choose to ‘edit settings’.
2. Under virtual hardware management you will see one or more network adapters.
3. Select the network adapter that you wish to assign to a different network
4. Select a different network from the drop-down menu

Your virtual machine is now part of a different virtual network. Keep in mind that the IP addresses of any devices that have been assigned to a different subnet also have to be changed.

Virtual Switch Configuration

The virtual switches are responsible for directing traffic throughout the virtual networking environment, and for keeping network segments separated. Although customized configuration of the virtual switches is possible, it is strongly advised not to manually configure these devices unless you have a thorough understanding of VMware and ESXi, as well as a clear and mapped out virtual network topology that you would like to implement.

To make changes to virtual switches, follow these steps:

1. In vSphere, go to the 'hosts and clusters' tab.
2. Select the host server (pre-configured to IP address 10.0.0.2).
3. Select 'configuration'.
4. Select 'networking'.
5. You now have an overview of the virtual switches that are directing traffic across the virtual network. You can add new network segments to these virtual switches, or remove and reassign them to other virtual switches. You can also connect or disconnect a virtual switch to a physical network adapter.

Once again, it is strongly advised not to change the virtual switch configuration unless you have a thorough understanding of VMware and ESXi, as well as a clear and mapped out virtual network that you would like to implement. Changes made to virtual switches may lead to your network not working properly.

NAT

Network Address Translation (NAT) with Port Address Translation (PAT) is already configured on the router. In other words, this service will work without any adjustments. The configuration is set to use the external facing interface on Vyatta. Thus, regardless of the address assigned for your public facing interface it will still function appropriately. The correct configuration will be the best choice for most businesses. Do not adjust the NAT rules unless it is required to meet specific needs and you have a thorough understanding of the procedure. Changes made to NAT may lead to your network being unable to properly access external resources.

To adjust NAT to translate to specific IP addresses, follow these steps:

1. 'set nat source rule [#] source address [x.x.x.x/x].
2. 'set nat source rule [#] translation address [x.x.x.x] || [x.x.x.x] – [x.x.x.x] || [x.x.x.x/x]'.

Once again, it is strongly advised not to change the NAT configuration unless you have a thorough understanding the procedure. Changes made to NAT may lead to your network not working properly.

Firewall Rules

If you follow the quickstart guide, your virtual router will have a firewall enabled with several base access control lists (ACLs) already pre-configured. The ACLs are as follows:

- Ingress
  - Only traffic from a session that has been initiated from the inside of your network is allowed into your network.
- Egress
  - Traffic sourced from VLAN 20 may not leave the external interface.
  - Traffic leaving the external interface must be destined for ports 80, 443, or 53.
- Screen Subnet
  - Traffic destined for VLAN 90 must have a destination port of 53.
  - VLAN 90 cannot communicate with VLAN 20.

Firewall rules are specific to each organizations policy. The firewall rules will have to be adjusted in most environments to meet your business needs. The most likely change will be an adjusted to the egress firewall rule to allow additional destination ports.

It is important to understand the fundamentals of ACL's before adding or removing any rules. Visit http://www.vyatta.com/downloads/documentation/VC6.5/Vyatta-Firewall_6.5R1_v01.pdf for in depth documentation on how to implement firewall rules with Vyatta. Listed below is the basic procedure for adding or removing firewall rules:

1. Create the firewall rule with the appropriate action
   a. set firewall name [name] rule [#] action [accept, drop, reject, inspect]
2. Choose which protocol to use.
   a. set firewall name [name] rule [#] protocol [protocol]
3. Define the address space.
   a. set firewall name [name] rule [#] [source, destination] address [x.x.x.x/x]
4. Define the ports.
   a. set firewall name [name] rule [#] [sourced, destination] port [#]
5. (Optionally) Configure which connection states are acceptable.
   a. set firewall name [name] rule [#] state new enable
   b. set firewall name [name] rule [#] state established enable
   c. set firewall name [name] rule [#] state related enable
6. Lastly, the firewall rule must be applied to the interface.
   a. set interfaces [int type] [int] firewall [in, out] name [name]

It is strongly advised not to thoroughly plan any configuration changes and to avoid doing so unless you have a thorough understanding of firewalls. Changes made to firewall rules may lead to your network not working properly.

Adding users to LDAP

To get the most out of your virtual network you'll want to add users to LDAP. LDAP creates a domain infrastructure similar to what Active Directory does under Windows. With LDAP, you can create groups and shared folders with access control so that only certain users and groups have access to certain resources.

The domain that is in use on your virtual network is 'sip.local'. You can change this domain to something more fitting to your organization. To do so, you'll need to log in to the SIP-SRV-LDAPDNS server and open up the web-based dashboard. On the dashboard, go to 'LDAP' where you can change LDAP settings.

Whichever domain name you choose, you'll want to add users and computers to this domain. Computers can be added individually, from each computers operating system. For information on how to add a certain computer and operating system to a domain, please review documentation specific for that operating system.

Adding users to a domain is done from within the SIP-SRV-LDAPDNS server. Log in to the server and open up the web-based dashboard. On the dashboard, go to 'users and groups'. Here you can add users and assign them to groups. If you also select the 'roaming profiles' option, every user can log in to every computer in your network and access the resources that you have assigned to them.

For more information on how to manage your domain, users, and groups under the Zentyal operating system, please review information on Zentyal at www.zentyal.com.